REMARKS

Reconsideration and allowance of the subject application are respectfully requested. Claims 1-14 remain pending.

Applicants appreciate the Examiner's withdrawal of the 35 U.S.C. § 101 rejection of claims 8-11.

Claims 1-14 are now rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,970,562 to Sandhu et al. in view of published U.S. Patent Application No. 2004/0103316 to Inada et al. This rejection is respectfully traversed. Specifically, as discussed in more detail below, Applicant respectfully submits that in addition to failing to teach or suggest formatting a calculated signature with the aid of the signature certificate received by the client station, Sandhu also fails to teach or suggest at least how a private/public key is generated, and how an electronic signature is calculated or how a cryptographic key is destroyed. Applicants further submit that the teachings of Inada fail to make up for these deficiencies.

The rejection will now be discussed in more detail.

As discussed in the Remarks of the previous Amendment, the embodiments of the present invention provide a system, method and software program for applying an electronic signature from a client station in a network. The client station is authenticated at a server of the network, and thus establishes an authenticated communication channel between itself and the server. The client then can generate a private key/public key pair, and send to the server, via the authenticated channel, a request for a signature certificate, generated by at least the public key. The client does not share the private key with the sever.

Upon receiving the request, the server sends a signature certificate to the client station, via the authenticated channel. The client station can then calculate a cryptographic

signature based on the private key, and then destroys the private key. The client station then formats the calculated signature based on the signature certificate received from the server via the authenticated channel.

The features described above are recited in amended independent claims 1, 8 and 12.

In the rejection, the Examiner contends that columns 3-4 of Sandhu teach features A through D recited in independent claim 1. Applicants respectfully disagree.

Sandhu teaches a system and method for crypto-key generation. Applicants respectfully submit that column 3, lines 22-33, on which the Examiner relies, teach the creating of a certificate for *public key encryption* to validate *public keys*. Applicants respectfully submit that this passage of Sandhu fails to teach or suggest the generation of a public/private key pair as explicitly recited in independent claims 1, 8 and 18 of the present application.

Furthermore, Applicants submit that column 3, lines 35-49 of Sandhu teach the revocation of public key certificates are part of the duties of the Certificate Authorities. Nowhere does this passage teach or suggest calculating an electronic signature or destroying a cryptographic key as the Examiner contends. Furthermore, Applicants submit that column 3, lines 50-67 of Sandhu teach split private key cryptography, not the creation or use of public keys. Column 4, lines 1-9 teach authentication by challenge and response with a symmetric key, and column 4, lines 10-19 teach authentication by challenge and response with an asymmetric key. Also, column 4, lines 20-33 teach SSL authentication using the signature of a message from the server side, and column 4, lines 33-42 teach SSL authentication using an authentication of the client by the server. Nowhere do these or any other passages of Sandhu teach or suggest destroying a cryptographic key after obtaining the signature as the Examiner contends.

Applicants further submit that one skilled in the art would not use a challenge/response authentication technique with symmetric keys as taught by Sandhu with a challenge/response authentication technique with asymmetric keys as also taught by Sandhu as the presumably Examiner contends in asserting that the symmetric key features discussed in column 4, lines 1-9 correspond to the features of step "B" in claim 1 while also asserting that the asymmetric key features discussed in column 4, lines 10-19 correspond to steps "C" and "D" of claim 1. Furthermore, even an attempt to combine the techniques was made, the claimed embodiments of the present invention would not be achieved.

Specifically, the Examiner contends that column 1, lines 1-33 teach that a client requests a signature certificate of a public key of the client as recited in step C of claim 1. However, Applicants submit that in SSL protocol, when the server signs a particular message to prove its identify (see column 4, lines 23-24 of Sandhu), the client uses the public key of the *server* to authenticate the signed message. Therefore, the client uses the chain of public key certificates to verify the public key of the *server*, that is, the certificate of the public key of the server as taught in column 4, lines 24-28 of Sandhu.

Accordingly, as demonstrated above, Applicants submit that Sandhu fails to teach at least the features of step C in independent claim 1, as well as the generation of a public/private key pair and the destruction of a cryptographic key as recited in step E of claim 1, and any corresponding features recited in independent claims 8 and 12.

Applicants further submit that Inada, which teaches an electronic document format control apparatus and method, fails to make up for these deficiencies in the teachings of Sandhu. Specifically, the Examiner relies on Inada merely for its alleged teaching of formatting a calculated signature. Applicants submit that nevertheless, Inada fails to teach or suggest, for example, the features relating to the signature certificate of step C in independent

claim 1, as well as the generation of a public/private key pair and the destruction of a cryptographic key.

For all these reasons, Applicant respectfully submits that one skilled in the art would have not found it obvious or possible to achieve the embodiments of the present invention even as defined in independent claims 1, 8 and 12 based on the teachings of Sandhu and Inada. Hence, all claims should be allowable.

In view of the above, it is believed that the application is in condition for allowance and notice to this effect is respectfully requested. Should the Examiner have any questions, the Examiner is invited to contact the undersigned at the telephone number indicated below.

Respectfully submitted,

/brian c. rupp/

Brian C. Rupp, Reg. No. 35,665
DRINKER BIDDLE & REATH LLP
191 N. Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698
(312) 569-1000 (telephone)
(312) 569-3000 (facsimile)
Customer No. 08968

Date: September 4, 2007

CH02/ 22496983.1